Journal of Number Theory 130 (2010) 1056–1060

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the size of the Gelfond exponent

Igor E. Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

ARTICLE INFO

Article history:
Received 22 July 2009
Revised 25 September 2009
Available online 7 November 2009
Communicated by Robert C. Vaughan

ABSTRACT

We use the explicit formula of V. Shevelev for the best possible exponent $\alpha(m)$ in the error term of the asymptotic formula of A.O. Gelfond on the number of positive integers $n \leqslant x$ in a given residue class modulo m and a given parity of the sum of its binary digits, to obtain new results about its behaviour. In particular, our result implies that

$$\liminf_{p\to\infty} \alpha(p) = 0$$

where p runs through the set of primes, which has been derived by V. Shevelev from Artin's conjecture.

1. Introduction

Let $s(n)$ denote the sum of binary digits of n. For integers $m > 1$, $a \in [0, m-1]$ and $\nu = 0, 1$ we denote by $T_{m,a,\nu}(x)$ the number of integers $n \leqslant x$ with

$$n \equiv a \pmod m \quad \text{and} \quad s(n) \equiv \nu \pmod 2.$$

As a very special case of a result of A.O. Gelfond [5] (which applies to sums of g-ary digits in a given residue class modulo d for arbitrary integers $d, g \geqslant 2$ with $\gcd(m, g-1) = 1$), for any odd m we have

$$T_{m,a,\nu}(x) = \frac{x}{2m} + O\left(x^{\alpha}\right), \tag{1}$$

E-mail address: igor@ics.mq.edu.au.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.09.005

where

$$\alpha = \frac{\log 3}{\log 4}.$$

Note that the above value of α does not depend on m.

V. Shevelev [9] has recently obtained a much more precise result giving an explicit formula for the best possible exponent $\alpha(m)$ in (1). That is, $\alpha(m)$ is a real number such that (1) holds for any $\alpha > \alpha(m)$ and fails for any $\alpha < \alpha(m)$. To formulate the main result of [9] we let t_m be the multiplicative order of 2 modulo an odd integer m. Then V. Shevelev [9, Theorem 1] gives the following explicit expression:

$$\alpha(m) = \max_{1 \leqslant a \leqslant m-1} \left(1 + \frac{1}{t_m \log 2} \sum_{k=0}^{t_m-1} \log \left|\sin\left(\pi \frac{a2^k}{m}\right)\right|\right). \tag{2}$$

This formula implies that if $m = p$ is prime and 2 is a primitive root modulo p then

$$\alpha(p) = \frac{\log p}{(p-1)\log 2}.$$

See [9, Theorem 2]. In particular, it is noticed in [9] that under the assumption of Artin's conjecture on primitive roots we have

$$\liminf_{p \to \infty} \alpha(p) = 0. \tag{3}$$

The purpose of this paper is to prove (3) unconditionally and in fact to show that $\alpha(p)$ is small for an overwhelming majority of primes p. Our result is based on the estimate of J. Bourgain [1] on exponential sums over small multiplicative subgroups, which in turn is an improvement of a result of J. Bourgain, A.A. Glibichuk and S.V. Konyagin [3], combined with an estimate on some products via exponential sums.

Throughout this paper, implied constant in the symbols O and $\ll$ may depend on the positive parameter ε and are absolute otherwise. We recall that the notations $A = O(B)$ and $A \ll B$ are both equivalent to the fact that there exists a constant c such that the inequality $|A| \leqslant cB$ holds.

Theorem 1. *For any $\varepsilon > 0$, there exist a set $\mathcal{R}_\varepsilon$ of primes p such that*

$$\#\{p \leqslant x:\ p \in \mathcal{R}_\varepsilon\} \leqslant \exp\left(O\left(\frac{\log x}{\log\log x}\right)\right)$$

such that for any sufficiently large $p \notin \mathcal{R}_\varepsilon$ we have

$$\alpha(p) \leqslant \exp\bigl(-(\log p)^{1-\varepsilon}\bigr).$$

2. Preparations

We recall the following estimate given in [1, Corollary to Theorem B].

Lemma 2. *For any $\delta > 0$, prime p and integer g with $\gcd(g, p) = 1$ of multiplicative order $t \geqslant p^\delta$ modulo p, the following bound holds*

$$\max_{1 \leqslant a \leqslant p-1} \left|\sum_{k=1}^{t} \exp\bigl(2\pi i a g^k/p\bigr)\right| \leqslant t p^{-\eta}$$

where

$$\eta = \exp(-C/\delta)$$

for some absolute constant $C > 0$.

We note that Lemma 2 allows us to choose δ as a slowly decreasing function of p, which is crucial for our argument.

We need the following result which is essentially [8, Bound (18.2)].

Lemma 3. *For any N complex numbers $z_1, \ldots, z_N$ on the unit circle, $|z_1| = \cdots = |z_N| = 1$, we have*

$$P \leqslant \exp\bigl(O\bigl(S \log(N/S + 1)\bigr)\bigr),$$

where

$$P = \max_{|z|=1} \left| \prod_{k=1}^{N} (z + z_k) \right| \quad \text{and} \quad S = \max_{\nu=1,\ldots,N} \left| \sum_{k=1}^{N} z_k^{\nu} \right|.$$

3. Proof of Theorem 1

Since

$$|\sin \vartheta| = \left| \frac{e^{i\vartheta} - e^{-i\vartheta}}{2} \right| = \left| \frac{1 - e^{2i\vartheta}}{2} \right|,$$

we rewrite (2) as

$$\begin{aligned} \alpha(p) &= \max_{1 \leqslant a \leqslant p-1} \left(1 + \frac{1}{t_p \log 2} \sum_{k=0}^{t_p - 1} \log \frac{|1 - \exp(2\pi i a 2^k / p)|}{2} \right) \\ &= \frac{1}{t_p \log 2} \max_{1 \leqslant a \leqslant p-1} \sum_{k=0}^{t_p - 1} \log \bigl|1 - \exp\bigl(2\pi i a 2^k / p\bigr)\bigr|. \end{aligned} \tag{4}$$

We now define $\mathcal{R}_\varepsilon$ as the set of primes p with

$$t_p \leqslant \exp\left(3\varepsilon^{-1} C \frac{\log p}{\log \log p} \right),$$

where C is the constant of Lemma 2. Then for $p \notin \mathcal{R}_\varepsilon$ we can apply Lemma 2 with

$$\delta = \frac{3\varepsilon^{-1} C}{\log \log p}$$

and thus with

$$\gamma = (\log p)^{-0.5\varepsilon}$$

that now implies that

$$\max_{1 \leqslant a \leqslant p-1} \left| \sum_{k=0}^{t_p-1} \exp\bigl(2\pi i a 2^k/p\bigr) \right| < t_p \exp\bigl(-(\log p)^{1-0.5\varepsilon}\bigr). \tag{5}$$

Therefore, recalling (4) and using Lemma 3 (with $z = -1$), we derive from (5) that

$$\alpha(p) \ll \exp\bigl(-(\log p)^{1-0.5\varepsilon}\bigr)(\log p)^{1-0.5\varepsilon},$$

that implies the desired estimate for a sufficiently large $p \in \mathcal{R}_\varepsilon$.

It remains to estimate the number of primes $p \in \mathcal{R}_\varepsilon$ up to x.

Let

$$T = \exp\left(3\varepsilon^{-1} C \frac{\log x}{\log\log x}\right).$$

Then

$$\#\{p \leqslant x\colon\ p \in \mathcal{R}_\varepsilon\} \leqslant \omega(W)$$

where $\omega(n)$ is the number of distinct prime divisors of n and

$$W = \prod_{t=1}^{T} \bigl(2^t - 1\bigr).$$

From the trivial inequality

$$\omega(n) \ll \frac{\log n}{\log\log(n+2)}$$

and using that $\log W \ll T^2$, we now obtain

$$\#\{p \leqslant x\colon\ p \in \mathcal{R}_\varepsilon\} \ll T^2$$

which concludes the proof.

4. Comments

We note that other estimates of exponential sums over subgroups of a finite field $\mathbb{F}_p$ of p elements can be used as well. For example, one can use estimates from [2,3,6,7] or any other bound which is nontrivial over a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of size $\#\mathcal{G} \leqslant p^{1/2-\eta}$ for some fixed $\eta > 0$. These bounds lead to much weaker estimates on the size of the exceptional set $\mathcal{R}_\varepsilon$ in Theorem 1, however the explicit bounds of [2,6,7] imply stronger upper bounds on $\alpha(p)$ for the remaining primes. In particular, one can obtain a series of trade-off results between the size of the exception set and the size of $\alpha(p)$ for the other primes.

We also note that the same technique can also be applied to estimating $\alpha(m)$ for integers m without small prime divisors.

Finally, we remark that Lemma 2 and the link between the discrepancy and exponential sums provided by *Erdős–Turán inequality*, see [4, Theorem 1.21] for its multidimensional version, imply that the fractional parts $\{a2^k/p\}$, $k = 1, \ldots, t_p$, are asymptotically uniformly distributed for any $p \notin \mathcal{R}_\varepsilon$

and integer $a \not\equiv 0 \pmod 1$. Then it may seem that now the *Koksma–Hlawka inequality*, see [4, Theorem 1.14], which relates average values of a function at uniformly distributed points with its integral average, may be applied to the function $f(x) = \log|\sin(\pi x)|$ and together with (2) leads to the desired result. This approach however fails at the above function $f(x)$ is unbounded as $x \to 0$ and thus the Koksma–Hlawka inequality does not apply.

Acknowledgments

The author would like to thank the anonymous referee for very careful reading of the manuscript. This work was supported in part by ARC Grant DP0881473.

References

[1] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, Geom. Func. Anal. 18 (2009) 1477–1502.
[2] J. Bourgain, M.Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields, Math. Proc. Cambridge Philos. Soc. 146 (2009) 1–21.
[3] J. Bourgain, A.A. Glibichuk, S.V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, J. Lond. Math. Soc. 73 (2006) 380–398.
[4] M. Drmota, R. Tichy, Sequences, Discrepancies and Applications, Springer-Verlag, Berlin, 1997.
[5] A.O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, Acta Arith. 13 (1968) 259–265.
[6] D.R. Heath-Brown, S.V. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Q. J. Math. Oxford 51 (2000) 221–235.
[7] S.V. Konyagin, Bounds of exponential sums over subgroups and Gauss sums, in: Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State Univ., Moscow, 2002, pp. 86–114 (in Russian).
[8] S.V. Konyagin, I.E. Shparlinski, Character Sums with Exponential Functions and Their Applications, Cambridge Univ. Press, Cambridge, 1999.
[9] V. Shevelev, Exact exponent in the remainder term of Gelfond's digit theorem in the binary case, Acta Arith. 136 (2009) 91–100.